MASTER OF SCIENCE
IN
COMPUTER SCIENCE

DEVELOPING A DISTRIBUTED NETWORK VULNERABILITY ASSESSMENT CAPABILITY THROUGHOUT THE DEPARTMENT OF THE NAVY.

Timothy J. Devlin-Major, United States Marine Corps
B.S., United States Naval Academy, 1988
Allen A. Harper-Captain, United States Marine Corps
B.S., North Carolina State University, 1995
Master of Science in Computer Science–June 2002
Advisor: Christopher S. Eagle, Department of Computer Science
Co-Advisor: Richard M. Harkins, Department of Physics

As the Department of the Navy grows more reliant on the capabilities of Network-Centric Operations, the vulnerabilities currently in our computer systems become critical vulnerabilities to the entire Naval Force.

The Navy's networks are under attack by a myriad of threats every day. The Fleet Information Warfare Center (FIWC) currently conducts vulnerability assessments of the Navy's unclassified networks, classified networks, and tactical networks. Additionally, FIWC has been tasked to conduct vulnerability assessments of the Navy and Marine Corps Intranet to ensure the contracted levels of security are being provided. It is time to take advantage of the Navy's most precious asset to offset the weaknesses presented by her network vulnerabilities. The professional Sailors and Marines, currently in IT billets throughout the fleet should be certified to evaluate their systems to find vulnerabilities and fix them prior to the threat. The development of a distributed vulnerability assessment capability will provide commanders the personnel to identify the risks associated with network operations.

This thesis examines the requirements to develop a distributed vulnerability assessment capability and proposes a certification process to accompany this capability. Finally, this thesis presents a unique and innovative on-line network laboratory that supports distance learning and certification not currently available elsewhere.

KEYWORDS: Computer Security, Information Assurance, Public Key Infrastructure (PKI), Networking

A DISTRIBUTED PASSWORD SCHEME FOR NETWORK OPERATING SYSTEMS

Christopher Roth-Major, United States Army
B.A., La Salle University, 1990
Master of Science in Computer Science-June 2002
Advisor: James B. Michael, Department of Computer Science
Co-Advisor: Craig Rasmussen, Department of Applied Mathematics

Password-based user identification and authentication in a network-based operating system generally relies upon a single file that contains user information and the encoded or hashed representations of each users' password. Operating system designers have resorted to various protection schemes to prevent unauthorized access to this single file. These techniques have proved vulnerable to various attacks, the result being unauthorized access to the targeted computer system. This paper proposes a model for a distributed password system in a network environment that eliminates the single password file as a target without introducing additional computational complexity or incorporating additional cost to the user with such items as tokens or biometrics. This application incorporates proven encryption techniques and a distributed architecture to enhance the reliability of an operating system's identification and authentication procedures. The paper provides an object-oriented model of this approach, along with an analysis of a possible implementation in a current operating system.

KEYWORDS: Password, Encryption, Attacker, Exploitation, Vulnerabilities, Security

REALISTIC SIMULATED AIRSPACE THROUGH THE USE OF VISUAL AND AURAL CUES

Robert E. Thien-Major, United States Marine Corps
B.A., University of Colorado, 1991
Master of Science in Computer Science-June 2002
Advisor: Rudolph P. Darken, Department of Computer Science
Second Reader: Joseph A. Sullivan, The Modeling, Virtual Evironments, and Simulation (MOVES) Institute

The increase in air traffic volume within the National Airspace System has prompted the Federal Aviation Administration to explore more efficient methods of conducting Air Traffic Control. Toward this end, a project to develop Simultaneous Non-Interfering (SNI) Routes for rotary wing aircraft has been undertaken. In order to develop these routes with an appropriate level of safety, the ability of a rotary wing pilot to fly an assigned path with the aid of Global Positioning System navigational equipment must be evaluated. This evaluation must be conducted initially in a simulated environment. So as to record the most accurate human performance data possible, the simulated airspace must be as close to reality as possible. The goal of this thesis is to accurately simulate the airspace for use in the development of SNI routes. In order to create a realistic simulated flying environment the performance and visual presentation of other air traffic was made to perform as they do in the real world. In addition, the radio transmissions heard by the simulator pilot were designed with both timeliness and accuracy with regard to the air traffic scenario. Through the use of these visual and aural cues, a realistic airspace simulation was created.

KEYWORDS: Simulated Airspace, Visual and Aural Cues

EXPLOITATION OF IEEE 802.11B NETWORKS: AN ELECTRONIC WARFARE PERSPECTIVE

Robert A. Vojtik-Major, United States Marine Corps
B.A., University of New Mexico, 1991
Master of Science in Computer Science-June 2002
Advisor: Tri T. Ha, Department of Electrical and Computer Engineering
Second Reader: Paul C. Clark, Department of Computer Science

As the use of wireless local area networks (WLANs) continues to increase in the United States and abroad, it becomes more important to have the ability to exploit this form of communication in both offensive actions to attack an adversary's network and defensive actions to protect our own infrastructure. This thesis examines the vulnerabilities within the IEEE 802.11b standard and the role of electronic warfare in exploiting this relatively new method of communication. It also recommends a set of tools and methods for exploiting IEEE 802.11b WLANs.

KEYWORDS: IEEE 802.11b, Wireless Local Area Networks, Exploitation, Electronic Warfare